

SECTION V. ESPIONAGE, SABOTAGE, LOSS , COMPROMISE, AND OTHER VIOLATIONS

5-100 Application. This section establishes the procedures for the conduct of administrative inquiries, investigations, and other administrative action required in connection with report of sabotage, espionage, and subversive activities; and the loss, compromise, suspected compromise, or security violations involving U.S. and foreign classified information (see paragraph 8-103c(4)).

5-101 Espionage, 1/ Sabotage and Subversive Activities.

a. On receipt of information from **any source** involving espionage, sabotage, or subversive activities not previously reported by a contractor in accordance with paragraph **6c, ISM**, the **CSO shall forward such information**, classified if appropriate, to the nearest field office **of** the FBI by the most expeditious means. A copy of all referrals shall be furnished to the Regional Director and the **Director, IS, ATTN:** Deputy Director (Industrial Security). The FBI will advise that office whether or not investigative jurisdiction is accepted and the **CSO** will be so notified. If the FBI declines investigative jurisdiction, the **CSO** shall initiate such other administrative inquiry or investigation of industrial security violations as may be indicated, or shall refer the case to appropriate **UA's** for disposition. If the FBI accepts jurisdiction, all such actions shall be deferred until completion of the FBI case. Reports of-completed FBI investigations will be made available to the CSO for review, forwarding to DISCO for evaluation of any unfavorable information disclosed, and determination as to whether or not additional investigation **and/or** inquiry is indicated. If during subsequent actions additional information is developed which is believed to be of interest to the FBI, a report shall be furnished-under the procedure outlined above for further FBI consideration.

b. On final disposition of the case by the FBI, the **CSO** through the Regional Director shall advise the Director, **DIS** and the appropriate **UA(s)** of all developments in the case.

1_/ See paragraph 5-104 for additional reporting requirements if the espionage involves conduct which comes or appears to come within the criminal sanctions of Chapter 37, Title 18, **U.S.C.** 537 (reference (w)) or of **§ 4** of the Subversive Activities Control Act of 1950 (Public Law 81-831, **§ 64** Statute 987, 989, 991, and 992, Chapter 1024) (reference (**ww**)).

5-102 Loss, Compromise 2/, and Suspected Compromise 3/.

a. On receipt of a report involving loss, compromise, or suspected compromise of classified information, including a preliminary report from a contractor in accordance with the requirements of paragraph 6a(2) and 7d, ISM, the CSO shall be responsible for the following.

(1) If the preliminary report indicates that other classified information may also be **in** danger of being compromised because of poor security practices or procedures, take immediate steps to ensure that adequate safeguards are established. This may involve an immediate visit to the facility to **ensure** that appropriate safeguards are established.

(2) If the **preliminary** report contains sufficient details to make a final determination in the case, advise the contractor **in** writing that no further investigation or report is required and then proceed in accordance with the procedures in paragraphs c and d below. *

(3) If the preliminary report does not contains efficient details to reach a final determination, establish a 15-day suspense for receipt of the final report from the contractor. More **time** may be allotted if necessary because of the **scope** or complexity of the inquiry.

(4) If the preliminary report deals with foreign classified **information, and** the security of such information is the responsibility of the Us., follow the procedures **in** paragraph 8-103c(4).

(5) If the preliminary report deals with commercial carrier CONFIDENTIAL shipments in transit, retransmit the report by electrical **means** within 24 hours of receipt to: Commander, Military Traffic Management Command, **ATTN: MTMC-SS, Nassif Building**, 5611 Columbia Pike, Falls Church, Virginia 20315.

b. On receipt of the contractor's final reports as to the results of his or her Inquiry, the CSO shall accomplish the following.

(1) Review the reports for adequacy.

2/ See paragraph 5-104 for additional reporting requirements if deliberate compromise of classified information **is** involved; that is, any intentional act done with the object of conveying classified information to any person not officially authorized to receive it.

3/ When the facility or contractor activity is located on a **UA** installation, and the Commander or Head of that installation is performing certain actions on **behalf** of the CSO, the action which this **paragraph** assigns to the CSO will be performed by the Commander or Head of the installation, except for that action prescribed in paragraph 5-102d(5) which shall remain the responsibility of the CSO.

(2) Conduct additional inquiry, if necessary. Normally the contractor's inquiry shall not be duplicated except as necessary to clarify issues or to obtain additional facts. The objective is to encourage **contractors** to make adequate investigations and to avoid duplication of Investigation. This does not negate the prerogative and responsibility of the CSO to initiate appropriate investigative action when necessary to safeguard classified information.

(3) Make a final determination that a loss, compromise, or suspected compromise did or did not occur.

c. If the final determination **is** made that a loss, compromise, or suspected compromise did not occur, the **CSO shall** ensure that the contractor has taken adequate action to prevent recurrence of such incidents.

d. If the final determination is made that a loss, compromise, or suspected compromise did occur, **the** CSO shall accomplish **the** following.

(1) Immediately furnish an advance notice with essential information to the UA contracting officers, including the ACO, so that action can be initiated to determine the extent of potential damage to the national security and to minimize the effect of the compromise **or** suspected compromise. The UA contracting officers should **also** be advised that a formal final report will follow. On receipt of the advance notification, the UA contracting officers should review the classification of the information involved for possible **downgrading** or declassification action. The CSO should be notified as soon as possible **as** to the results of the classification review and the action taken or initiated to mitigate **the damage to** national security. The CSO shall continue the ensuing processing without waiting for a reply from the UA contracting officer(s) if undue delay is encountered.

(2) Make a 'determination as to whether a weakness in security practices or procedures caused or permitted the loss, compromise, or suspected compromise, and ensure that such practices and procedures are revised to prevent recurrence.

(3) Make a determination as to whether individual responsibility can be fixed for the loss, compromise, or suspected compromise, and recommend **denial** or suspension of clearance, when appropriate, **in** accordance **with** paragraph 2-320.

(4) Make a determination as to the contractor's responsibility for the loss, compromise, or suspected compromise and recommend, when appropriate, action In accordance with paragraph 4-201.

(5) Make a determination in the case of lost classified material for which the contractor **is** unable to provide accounting as to whether the contractor's accountability for the classified item(s) **should** be terminated. If the circumstances of the case indicate that an adequate and exhaustive search has been made, and additional effort would not be expected to lead to **the** recovery of the material **or** provide a probable explanation of the **manner** of loss, the CSO shall direct the contractor. to terminate accountability for the classified material **in** accordance with paragraph 12b, ISM. **An** information copy of the **letter** directing termination of accountability shall be forwarded

to the contracting officer concerned. If the contractor subsequently locates or recovers the classified item, a report shall be submitted to the CSO in accordance with paragraph **6a(16)**, ISM. Upon receipt of such report, the **CSO** shall notify the contracting officer concerned.

(6) Prepare a final report for record purposes. Where the investigation has been conducted **by** the commander or head of a UA installation in accordance with paragraph **1-108b**, his or her **final** report will be forwarded to the CSO concerned for processing. The report will be addressed to the UA contracting officer, and a copy shall be forwarded to the ACO. A copy of the report shall be forwarded to the Director, **DIS, ATTN:** Deputy Director (Industrial Security) in any case where TOP SECRET information is involved. If **COMSEC** material is involved, a copy of the report **will** be furnished to the COR **as** required by paragraph 24 of DoD 5220.22-S-1 (reference (q)). The report, which **shall** enclose a copy of the final report of inquiry or a complete and detailed **summary** thereof, shall be prepared in the following format.

(a) Authority. Cite the reason for the inquiry including when, where, and by whom it was conducted.

(b) Essential Facts. Arrange facts (not opinions or assumptions) in chronological order. Avoid trivialities. Conflicting **assertions of** fact should also be discussed.

(c) Corrective Action. Specific action taken to preclude a recurrence of similar incidents and the disciplinary action, **if** any, taken against responsible individuals.

(d) Conclusions." Summarize conclusions reached as a result of the facts, and provide an analysis' of all pertinent information bearing thereon. It is desirable, in the matter of arrangement, that the conclusions follow the sequence of the reported facts. If the conclusions of the CSO differ from a contractor's conclusions, a rationale shall be furnished.

(e) Recommendations. Include all actions required to effect disposal of the case. The recommendations shall be consistent with the conclusions. Identify those **recommendations** considered beyond the scope of authority of the CSO. .

(f) The report shall reference the results of the review action taken by the UA contracting officer(s) with regard to downgrading or declassifying the information and mitigating the damage to national security. If the results are not known at the time of submission of the report, this fact shall be so indicated, and **a** copy requested when completed.

5-103 Investigative Support.

a. The CSO **shall request professional** investigative support from **one of** the three **military** departments when a case **falls** under the following criteria:

(1) any case which involves RESTRICTED DATA or FORMERLY RESTRICTED DATA, in which the CSO suspects that a criminal violation-of the Atomic Energy Act of 1954 (reference (o)), as amended, has occurred; or

(2) a need exists for special investigative techniques.

b. When a case meets the above criteria, the case file together with a copy of available reports, shall be referred to the investigative agency of the military department which awarded the contract. If the contracting military department cannot be **ascertained**, or if more than one department is involved, the investigative agency of **the** military department **having** the principal procurement interest in the facility will assume investigative responsibility. Requests of the Office of Special Investigations, USAF (OSI) **and** Naval Investigative Service (NIS) investigative services shall be routed to the local **field** office **servicing** the geographical area in which the facility is located. Requests for **Army** investigative services shall be routed to the **COMMANDER, U.S. Army Intelligence and Security Command, ATTN: LAOP-OP, Fort Meade, Maryland 20755.** An information copy **of** such referral shall be sent to the contracting officer of the **UA's** concerned, the Regional Director, **am!** the Director, **DIS**, ATTN: Deputy Director (Industrial Security).

5-104 Additional Reporting **of** Espionage, Criminal Activity, and Deliberate Compromise Cases.

a. DoD instruction 5200.22 (reference (xx)) requires the reporting by the most expeditious means possible under the circumstances of every incident in defense industry in which espionage, **criminal** activity, or deliberate compromise is suspected or believed to have occurred. (Criminal activity refers to conduct that **is** or may be a violation of a **federal or** state criminal law, The Uniform Code of Military Justice, the common **law, and, in** addition, the criminal laws of foreign countries which might embarrass or **otherwise** be of concern **to** the DoD. Selective judgement should be exercised in determining what matters are to be reported, based on such factors as the nature of the criminal act, the **clearance** level of the individual concerned, and his or her relative position **in** the company.) When the full report required by paragraph b below would cause undue delay, **an** interim report containing information immediately available will be submitted.

b. When a case falls within the **purview** of this paragraph, the CSO, in coordination with the contractor concerned, contracting officers(s), investigative agencies, the Commander or Head of the UA installation performing security actions under the provisions of paragraph **1-108b** and DISCO shall **submit** a report to the Director, DIS, ATTN: Deputy Director (Industrial Security) containing the following minimal information:

.(1) identification of the persons involved together with a brief summary of their backgrounds including the **name** and address of the contractor who employs them and their **PCL's** -- the report shall include advice as to any action that has been taken or recommended with respect to revocation, suspension, or withdrawal of the individual's PCL;

(2) the category of classified information involved and an estimate of **the** time the information will retain such sensitivity;

(3) . description of the classified information **involved**;

(4) evaluation of the significance to the national security of the classified information which was or might have been compromised;

(5) summary of the circumstances of the actual or attempted compromise;

(6) copy of any report of investigation, final or interim, conducted in connection with the compromise;

(7) evaluation **of** the compromise to indicate any area of security weakness exposed by the compromise;

(8) report of any change in the procedures of the contractor resulting from the compromise, and recommendations for any changes **in** the DoD Industrial Security Program that might prevent future compromises of a similar nature; **and**

(9) advice as to whether disciplinary action has been taken or is recommended, or whether the incident has been referred to another federal department for appropriate further action.

c. When a case involves criminal activity, the following **information** shall be furnished:

(1) full identification of persons involved to include full name, date and place of **birth**, local address, and present whereabouts;

(2) facts concerning **actual** or attempted crime;

(3) pending or completed action **in** court or other tribunal including disciplinary action taken or recommended;

(4) a copy of any report of investigation, final or interim, conducted **ed** in connection with the crime or charge; **and**

(5) a statement as to why it is believed the incident might embarrass or otherwise be of concern to the DoD.

d. On receipt of a report as described above, the Director for Industrial Security, **shall review** it for adequacy, resolve any inconsistencies, and transmit the report through the Director, **DIS** to the Director, Counterintelligence and Investigative Programs, DUSD (P), with appropriate comments.

5-105 Other Security Violations **4/**.

a. On receipt of a preliminary report from a contractor in accordance with the requirements of paragraphs 6a(3) and 7d, **ISM**, or a report from a

4/ If **this** type of violation also involves the loss, compromise, or suspected compromise, the procedures in paragraph 5-102 apply.

government source, the CSO shall determine whether the circumstances involved in the violation warrant further investigation by the contractor or an administrative inquiry by the **CSO**, or whether the preliminary report is considered sufficient. In the latter case, advise the contractor, in writing, that no further investigation or report is required. The facts uncovered **shall be** evaluated **and** a final determination made as **to** what action is required by the contractor to preclude the possibility of similar violations in the future. A formal report of violations to other organizations is not **required**, unless the preliminary report was received from a government source. In such a case, the government source will be advised of the results of the inquiry.

b. If the violation involves classified **COMSEC** information (but not loss, compromise, or suspected compromise), a report shall be submitted by the **CSO** to the UA contracting officer and the **COR** as required by paragraph 24 of reference (q). A copy of the report shall be furnished **to** the Director, **DIS**, **ATTN** : Deputy Director (Industrial **Security**).

5-106 Other Administrative Violations.

e. When a report is received from a contractor, in accordance with paragraph **6a(9)**, **ISM**, that an employee refused to execute a security briefing and termination statement, the **CSO** shall accomplish the following.

(1) If possible, contact the former employee by letter or **tele-**phone and arrange for the former employee to execute the security termination statement and return it to the CSO.

(2) In connection with subparagraph (1) above, the CSO shall recover any classified material in the possession of the former employee.

(3) If the former employee does execute the DISCO Form 482, the form shall be **forwarded** to the **former employer** -- no further action is required.

(4) If the action taken in accordance with subparagraph (1) above is not successful, the **CSO** shall review the circumstances in the case. If the former employee cannot be located and circumstances suggest that the apparent disappearance may be of security significance, the FBI **shall** be notified. The CSO **shall** advise DISCO in all **cases** of refusal to sign the security termination statement, **or** whenever the former employee cannot be contacted or located. DISCO **will** record such information in the **PSCF**. If DISCO subsequently receives a request for a new PCL for the individual, the request **will** not **be** processed until the individual executes the security termination statement **or** provides an acceptable reason for refusal.

b, When a report **is** received from a contractor in accordance with paragraph **6a(10)**, (11), or (12), **ISM**, and paragraph **1-703b** concerning a **delay** in a classified shipment, evidence of tampering with a classified shipment, or delivery of a classified shipment by unauthorized methods, the CSO will conduct additional inquiry, if appropriate, to ascertain the facts. Such inquiry could entail contact, either personal or by correspondence, with the consignor, consignee, or the carrier involved. A report of the facts, conclusions, and **recommendations shall** be submitted to the contracting officer and Director, **DIS**, **ATTN**: Deputy Director (Industrial Security), for review and further

action with copies to the Regional Director. If a shipment containing **classified** information was tampered with, advise that office what law enforcement officials were notified, if any.

5-107 Responsibility of Contracting User Agency to Investigate Certain Breaches of Security.

a. When an unauthorized public disclosure of classified Information **is** discovered and it is not possible to determine whether it **emanated** from a government or industrial source, the contracting **UA** responsible for the information shall initiate promptly an investigation of such breach of security in order to determine the cause and establish responsibility. If a government source **is** involved, the contracting **UA is solely** responsible for ensuring adequate corrective action to prevent future compromise of this nature.

b. If the unauthorized public disclosure was from an industrial source (normally a violation of paragraph **5o**, p, or q, **ISM**), the contracting **UA** will request the **CSO** to bring to the attention of the contractor the corrective action that should be taken to prevent future compromises **of** this nature.

c. If the situation warrants, **the** contracting **UA** will request **the** Director, **DIS**, to take appropriate measures against **the** contractor, **including** the revocation of the FCL in the most extreme **cases**. Also, the revocation or suspension of **PCL's** of contractor employees involved in the security breach, **as provided** for **under** the provisions of paragraph 2-320, may be recommended by **the** contracting **UA**, in which case the Director, **DIS**, will take the required administrative action.

d. The contracting **UA will be** responsible for furnishing **any additional** information required by **DISCR**, as the result of action taken **in** paragraph c above.

e. Action to terminate existing contracts with the facility shall be the sole responsibility of the contracting **UA**.

5-108 Inquiries into Delays, Tampering, or improper Shipping Methods.

a. When, **in** accordance with paragraph **6a(10)**, **ISM**, the **CSO is** notified **that** a **SECRET** or **CONFIDENTIAL** shipment has not been received by the consignee within **48** hours **after** the expected time of arrival, the **CSO** shall **ensure** that the consignor has requested the carrier to trace the movement of the shipment and is otherwise making every reasonable effort to determine the whereabouts of the shipment. Additionally, only **if** the shipment was **CONFIDENTIAL**, the **CSO** shall provide a copy **of the** report to the Commander, **MTMC**, as outlined **in** paragraph 5-102a(5). If all efforts to **locate** the **shipment** are unproductive, the consignor shall be requested to furnish a full report of the incident, including any and **all** circumstances surrounding the incident. Normally the consignor **shall** expend no more than **72** hours **to locate** the shipment. The **CSO shall** then take appropriate action **in** accordance with this section.

b. When, **in** accordance with paragraph **6a(n)** or **(12)**, **ISM**, the **CSO** is notified of evidence of **tampering** with the shipment or of receipt of classified **material** by other **than** approved methods, the **CSO** shall conduct

appropriate inquiry only: (i) when the contractor's report of inquiry is considered inadequate, or (ii) the contractor's report is insufficient to support the contractor's conclusions that a compromise of the classified contents did or did not occur. In order to prevent a recurrence of the incident, a copy of the report received under paragraph **6a(12)**, ISM, shall be routed to the CSO of the contractor determined to be responsible for the violation, unless both the sending and receiving facilities are under the cognizance of the same office. If **the** violation was committed by a UA activity, a copy of the report shall be sent to the Commander or Head of the activity concerned.

c. The CSO shall analyze the reports required by paragraph a or b above, to determine if a particular-carrier **is** responsible for delays **in** the shipment, or if a series of incidents relating to failure to comply with the shipping instructions has occurred. A record shall be maintained to identify the carrier involved. When the record shows an accumulation of reports regarding a particular carrier, the **CSO** shall, if the carrier **is** a cleared facility, conduct a comprehensive inspection of the **carrier's** procedures for handling a classified shipment. Recommendations for corrective action shall be submitted to the carrier if the carrier is a cleared facility, or to **MTMC via** the Director, DIS, **ATTN:** Deputy Director (Industrial Security), if the carrier is an uncleared **facility**. Failure of a cleared carrier to take appropriate corrective action will be considered as the basis for a recommendation for revocation **of** the **FCL** of the carrier.